<Policy Topics> 非営利組織などの小さな組織の情報セキュリティポリシーの策定の試み

Policy Topics

非営利組織などの小さな組織の情報セキュリティポリシーの策定の試み[1]

Attempt to Develop an Information Security Policy for a Small Organization Such as a Non-profit Organization

会田　和弘[2]
Kazuhiro Aida

1．はじめに

ここ数年の情報セキュリティのインシデントを振り返ると、非営利組織であっても被害にあう可能性は大きく、組織的にセキュリティ対策を整備することが求められているように思える。しかし、非営利組織がセキュリティポリシーを策定しそれを実行している例は非常に少ない。それは、非営利組織の意識の低さというよりも、セキュリティ対策に通じていないや対策費用の不足、そしてセキュリティポリシー構築がパッケージ化されていないことなどが考えられる。

そこで、2020年4月から2つの非営利組織に対して、セキュリティポリシーの策定とその実施手順を整備する試みを行った。その概略をここで紹介したい。

2．非営利組織の現状は改善が必要

非営利活動は、社会的差別、固定化した貧困、難病、高齢者介護、まちづくりに関わる社会的課題を解決し不特定かつ多数のものの利益の増進に寄与することを目的とする活動[3]である。2021年4月末の時点で、法人格を有するだけで50,820団体、任意団体や運営形態にこだわらない活動もあり、さらに活動内容も規模も様々でその全体像を明確にすることは難しい[4]。

ありがたいことに、日本のほとんどの地域に、困っている人に寄り添い助けてくれる人たちがいる。その非営利組織は、ミッションを達成する為に、困っている人の個人情報やプライバシーに関わる情報を扱っている。例えば、致し方ない理由で不正滞在になってしまった外国人、難病に苦しむ人、家庭内暴力で悩む主婦、コロナ禍で仕事を失ったシングルマザーなどへの支援には、本人だけではなくその同居者についての機微な情報を扱わざるを得ない。その情報は、行政であれば生体認証などで高度なアクセス制限が施された基幹システムで管理されるべきものである。そのような情報を、個人のパソコンに入れ支援活動を行なっている場合も、非営利組織では珍しくない。

他方、狙われるのは多くの顧客情報をもつような企業であって、小さなそれも非営利組織は攻撃の対象にはならないだろうという見解もある。し

1　本稿は2020年12月14日（月）本学神戸三田キャンパスでの講演をもとにしたものである。

2　認定特定非営利活動法人イーパーツ常務理事　東京電機大学サイバーセキュリティ研究所研究員　千葉大学工学部・成蹊大学理工学部非常勤講師

3　特定非営利活動促進法では、NPO法人の20活動分野を定めている。当該法律はhttps://elaws.e-gov.go.jp/document?lawid=410AC1000000007、そこで定められている活動分野はhttps://www.npo-homepage.go.jp/about/toukei-info/ninshou-bunyabetsuを参照。

4　特定非営利活動法人数は、内閣府NPOホームページ「認証・認定数の遷移」による。https://www.npo-homepage.go.jp/about/toukei-info/ninshou-seni また、内閣府（2018）によると特定非営利活動法人の非営利活動の事業規模は、平均で3,086.2万円、中央値で942万円である。活動費が足りない場合、個人からの借り入れに頼っている。また、職員数の平均は12.1人、中央値は5人である。他のデータをみても、特定非営利活動法人の大半は零細企業と同等の経営であるとみて良い。ここでは、特に断りがない場合は、法人格の有無に関わらず、NPO法人の20活動分野で非営利活動を実施している団体を「非営利組織」と呼ぶこととする。

かし、昨今、中小企業も攻撃の対象になっている。それは、情報セキュリティ対策が手薄な中小企業のコンピュータに侵入し、そこから不正取得した取引会社の担当者などの情報を足がかりにして、さらにその取引会社のコンピュータに侵入…を繰り返し、遂には大企業のコンピュータ侵入を試みる攻撃が報告されている。これは、大企業のサーバの防御が厳しくなったことから、サプライチェーンにおける脆弱な部分を狙ったものである。これを、非営利組織と行政との協働に重ね合わせれば(図1)、小さな非営利組織が狙われる可能性がある[5]。もし攻撃に合えば、支援を必要としている人たちのセンシティブな情報も外にでることとなる。最悪の場合は、ダークネットで売買される可能性もあるだろう。

ところで、情報セキュリティの世界では、インシデントの発生可能性は脅威と脆弱性と情報資産の積と定義されている。この観点と非営利組織の現状を考慮に入れると次のように課題を整理できよう。

① 重要な情報やセンシティブ情報をもっている(重要な情報資産の存在)
② サプライチェーン攻撃の観点から、小さな非営利組織を狙う攻撃者がいる(脅威の存在)
③ 非営利組織は小さな組織は、総じて、情報セキュリティ対策があまい(脆弱性の存在)

つまり、非営利組織は情報セキュリティ上大きな課題を抱えていることになり、それを解消するには、早急に③の情報セキュリティ対策を整備する必要がある。

では、非営利組織側はこの状況に気がついているのだろうか。2020年に日本NPOセンターが1300余りの非営利組織に対して実施した調査結果によれば、86%が組織内でのデータ共有が進んでいる

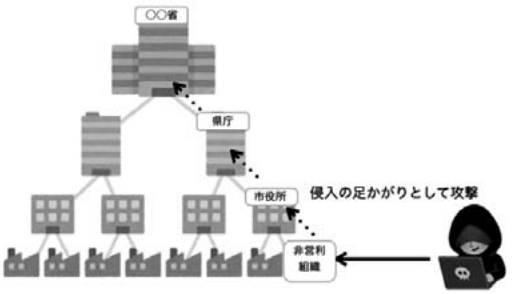

図1. 防御が甘い非営利組織をまず狙い、行政への侵入を目指す。

一方で、情報セキュリティ対策がとられているという回答は37%に過ぎない。将来セキュリティ対策を強化していきたいという組織は43%であった[6]。この調査の質問項目では情報セキュリティ対策の具体的な内容が明確ではなく、対策の実態に明らかにするデータとは言えないが、非営利組織が情報セキュリティ対策に関心をもっていることはどうやら確かなようである。では、情報セキュリティ対策が進まない原因は何か。人材と費用にあると同報告書はいう。これは、この報告を待たずに以前より様々な報告書で指摘されている。中小企業のセキュリティ対策の遅れも同じ理由である。もしこれに付け加えるとすれば、情報セキュリティ対策が最先端のビジネスでありドル箱であり、非営利組織への支援としてはなかなか無償では提供しにくい面もあるのだろう。

3．ISO27000の壁

非営利組織の実態を探るべくアンケートとヒアリングを独自で行ったところ、次のような実態が見えてきた。

・ 実施している情報セキュリティ対策は、スタッフ個人が行うアップデートおよびセキュ

5 2017年に発覚して日本年金機構情報漏洩事件も、厚生労働省を本丸として狙う攻撃の過程であり、日本年金機構の共有サイトに150万件の個人情報が内部規約に反して保存されていたことで、漏洩事件に繋がったということはよく知られている。この事件については、「調査結果報告 - 日本年金機構(平成27 年8 月20 日)」を参照のこと。
6 日本NPOセンター(2020)「非営利団体における IT 活用と IT 人材の実態及び、STO に対するニーズに関する調査」による。

リティ対策ソフトの導入と運用、パスワードの管理が主である。

- EMOTETなどの特定のマルウェアや攻撃が広がっていることに対しての注意喚起も、同僚を通じてインフォーマルに伝えられることはあるが、組織からの公式なものはない。
- 組織にセキュリティポリシーがない。あってもWebに公開されている基本方針のみである。そもそもセキュリティポリシーを理解していないことが多い。業務マニュアルに特定の情報にアクセスする権限が定められていることはある。
- 情報セキュリティ対策を進める専門部署および専任の役員が不在であることが多い。大半は、組織の中で比較的PCに詳しい総務担当者が兼任している。この担当者は、情報セキュリティ対策について専門の教育を受けたことがない場合がほとんどである。
- 偽装メールの添付をクリックした場合など、インシデントが発生した際の通報先が定められていない、またはあっても周知されていない。
- 情報セキュリティ対策についての予算は、セキュリティ対策ソフトのライセンス費用程度で、人件費は確保されていない。

これに対して、ISO27000等では、情報セキュリティ対策の重要な柱として、次の点を要求している。

i. 対策基準すなわち実施すべき対策を明確にすること
ii. その対策をPDCAサイクルで実施すること
iii. 担当役員をトップにすえ、各部署の代表者からなる全社的組織をつくり、それが主導で上ｉおよびｉｉを実施すること

iの対策基準を作成する手順は図2に示す。まず

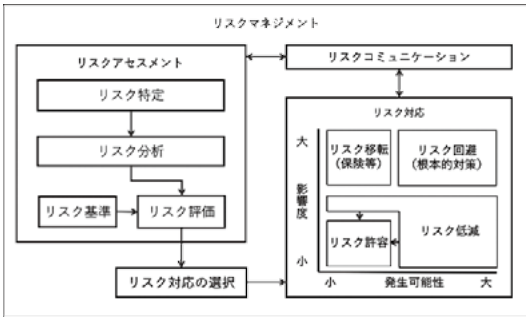

図2. ISO27000　リスクマネージメント

扱っている情報のリスクを洗い出し評価する（リスクアセスメント）、リスク値を下げるように対策基準を策定する（リスク対応）、そして、これらの手順と結果をスタッフと共有し（リスクコミュニケーション）必要があれば改定する。

この図2の複雑な過程は、専門の担当者がいる大企業のみが実施可能であると言ってよい。しかし、昨今の攻撃の実態から中小企業向けの対策も重要視され、IPAは「中小企業向けの情報セキュリティ対策ガイドライン第３版」[7]を公開した。

このガイドラインは、図2による対策基準の策定ノウハウを明らかにすると共に、付属しているエクセル表（情報管理台帳）を使えばリスク値を計算でき、その結果脆弱性が明らかになり対策基準を策定できるものである。その過程の一部を図3に示す。また、担当役員がいかに重要な役割を果たすか、予算を確保することの重要性、PDCAで対策を維持することも同ガイドラインにまとめられている。

これらの手法は、中小企業がISO27000の要求を満たす対策をとる為の道筋である。しかし、どのくらいの中小企業が図3を実施できるだろうか。ましてや、より経営が厳しくかつ慢性的な人材不足に悩む非営利組織にとってはさらに難題である。

7　https://www.ipa.go.jp/files/000055520.pdf

図3. IPAの「中小企業向けの情報セキュリティ対策ガイドライン」を用いたリスク値

サイクル	セキュリティポリシー		専門家の介入
Plan	対策基準の策定	既存の基準(ベースライン)の選出と、その中から実施可能な対策基準の選出。	セキュリティ対策委員会と次の1年の目標を設定。
Do	対策の実施	実施可能な方法で対策基準を実施する。その際、無理がなく実施できる方法を選択し、継続できるようにする。	インシデント等が生じた場合のアドバイス。
Check	対策の実施状況の確認	スタッフにアンケートまたは小テストを実施し、組織のセキュリティレベルの測定。スタッフ、役員へのヒアリング。	アンケート項目、小テスト、ヒアリング項目の作成。
Action	改善点の洗い出し	情報セキュリティ対策として追加できそうなものを選出。対策が遵守されなかった点は実施方法を改善する。新たに追加された情報や法律への対応。	セキュリティ対策委員会とのテストおよびヒアリング結果を検討。

表1. 小規模非営利組織向けPDCAサイクル

4．できることから積み上げる対策

このように小さな非営利組織が独力でセキュリティ対策を策定することはまず不可能である。とは言え、外部に常事支援を委託するにしてもその費用を捻出することも難しい。そこで、先にあげたガイドラインに付属している「新5分でできる！　情報セキュリティ自社診断[8]」を利用し、次のように対策を進めた。

（ア）　セキュリティ対策委員会を創設。本来は役員が委員長をつとめることが望ましいが、総会での承認が必要などで期途中からは難しいことが多い。

（イ）　現在のセキュリティ対策を進めようとしているスタッフを中心に複数名からなる組織をまずつくり、「一人ではやらせない」という体制をつくる。

（ウ）　PDCAを表1のように組み立て、専門家の介入をピンポイントとした。

（エ）　対策基準は、上で示した方法で策定したが、具体的には下記の流れでおこなった。

(1)　情報管理台帳の作成をまず行う。これは、今回の対策基準策定には直接使用しないが、将来今本格的にリスク分析を行う上で情報管理台帳は必

8　https://www.ipa.go.jp/files/000055848.pdf

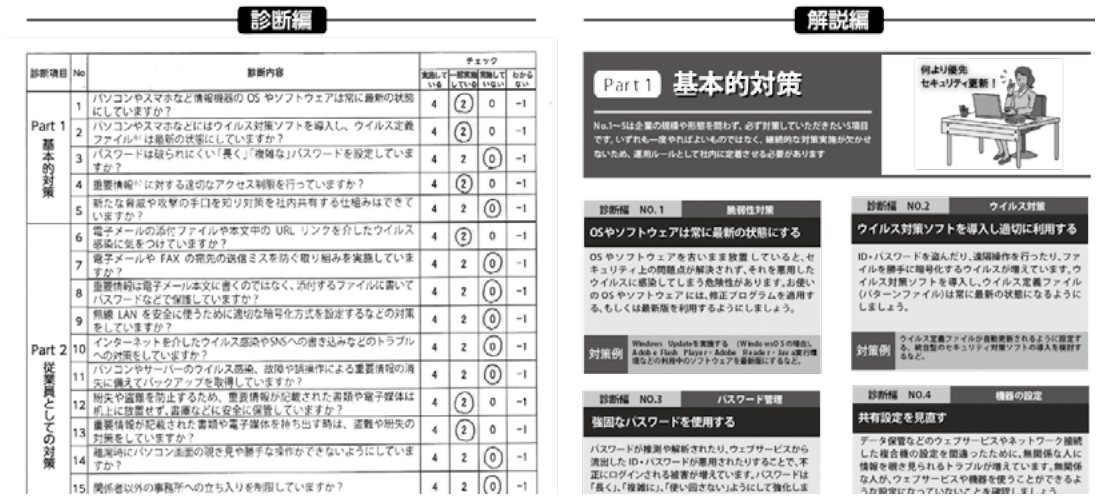

図4. IPA「新5分でできる！　情報セキュリティ自社診断」の診断編と解説編

要不可欠であることを見越してでもあるが、むしろ自分たちがどのような情報をもっているかを共有することが重要であるからである。

(2) IPAの「新5分でできる！　情報セキュリティ自社診断」の診断編をスタッフに対して実施。その結果を図4に示す。今回対象とした団体は、情報セキュイティ対策には積極的な団体であったにも関わらず点数が低い。これは、担当者レベルはそこそこでも、組織全体へ対策が浸透していない、組織としてスタッフへのコントロールが十分でないことによる[9]。

(3) セキュリティ対策委員会と協議し、「まずは基本的対策を４に」などと実施する対策に優先順位をつける。その際、その対策内容とともに、その実施方法も実行可能なものか検討する。例えば、ルールブックを配布するだけではなく、その内容を少しずつ朝のミーティングで他の連絡事項と一緒に「パスワードの長さ」についても伝えるなどである。スタッフの反応もここで把握でき、必要に応じて対策基準を変更する。

(4) 対策基準に盛り込まれるのは、基本的な対策としたが、非営利組織に特有な私物PCの扱いや「怪しいメールの添付をクリックした場合はこちらに連絡」などインシデント対応に関わるものは基本的なものではなくても積極的に盛り込む必要がある[10]。

(5) 以上で定めたルールブックとし文書化する。

(オ) 最後に組織がなぜ情報セキュリティ対策に取り組むかを示した「基本方針」を作成しWebに掲載した。

9 この段階はリスクアセスメントのリスクの特定とリスク分析にあたる。ISO27000でも、多くの企業に共通している点はチェックリスト方式のリスク特定や詳細リスク分析の計算を行わず出来合いのものを使用するベースラインアプローチなどが認められている。今回はIPAの「新5分でできる！」の診断編でリスク特定し、それをもとに専門家がリスク分析を行った。

10 (1)～(3)がリスクアセスメント、(4)～(5)がリスク対応にあたる。また、リスクコミュニーションは(3)に盛り込む。

なお対策基準の見直しは、まず「新5分でできる！」をスタッフ全員に行いその結果をもとに検討する。実施可能なものを新たにルールブックに追加し、「新5分でできる！」の25項目すべてが盛り込まれた時点で、より本格的なセキュリティポリシーへ次のステップに移行することとなるだろう。

5．おわりに

以上作成したルールブックは、その手順は一応ISO27000の意図を汲んでいるが、非営利組織らしく手作り感満載で標準的なセキュリティポリシー[11]とは異なったものとなった。しかし、適切なセキュリティポリシーとはなんであろうか。それは、スタッフにとってわかりやすく、それで組織がどのようにセキュリティ対策を進化させていくのか、その道筋がデザインされていることが必要であろうと思う。

できたものを上から押し付けるのではなく、徐々に対策基準をその実施方法とともに追加していくこの形は、まさに走りながら考える非営利組織の動きにはあっているように思える。現在、昨年度策定したポリシーのCheckとActionの時期である。対策基準の実施と改善は担当者の努力もあり順調である。その一方課題は、役員がどれだけ情報セキュリティ対策に責任を持てるかである。彼らが理解できないことは団体のルールにはならない。そう考えると、役員向けの情報セキュリティ対策の教育コンテンツが必要になってくる。それは今後の課題としたい。

【参考文献】

内閣府(2018)「平成29年度特定非営利活動法人に関する実態調査報告書」
https://www.npo-homepage.go.jp/uploads/h29_houjin_houkoku.pdf
日本NPOセンター(2020)「非営利団体における IT 活用と IT 人材の実態及び、STO に対するニーズに関する調査」
https://www.jnpoc.ne.jp/wp-content/uploads/2020/12/JNPOC_report.pdf
日本年金機構不正アクセスによる情報流出事案に関する調査委員会(2015)「不正アクセスによる情報流出事案に関する調査結果報告」
https://www.nenkin.go.jp/info /index.files/kuUK4cuR6MEN2.pdf
IPA(2021)「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
IPA(2019)「新5分でできる！　情報セキュリティ自社診断」
https://www.ipa.go.jp/files/000055848.pdf
JNSA(2016)「情報セキュリティポリシーサンプル改版(1.0版)」
https://www.jnsa.org/result/2016/policy/

11　JNSA「情報セキュリティポリシーサンプル改版(1.0版)」https://www.jnsa.org/result/2016/policy/